202 KAR 6:030. Confidential and proprietary information.

RELATES TO: KRS 65.7621-65.7643, 47 U.S.C. 153(27), 332(d)
STATUTORY AUTHORITY: KRS 65.7633(1), 65.7639
NECESSITY, FUNCTION, AND CONFORMITY: KRS 65.7633(1) requires the CMRS Board to implement the provisions of KRS 65.7621 to 65.7643 through the promulgation of administrative regulations. In order to comply with KRS 65.7629, 65.7639, and administrative regulations promulgated by the CMRS Board, it is necessary that the board and PSAPs (public safety answering points) certified by the board obtain proprietary information. KRS 65.7639 protects such information and governs the form and manner of its release to others. This administrative regulation establishes the procedures by which the board shall insure the security of confidential or proprietary information.

Section 1. Identification of Confidential or Proprietary Information. (1) Information identifying subscribers shall be held confidential, as proprietary information belonging to the disclosing CMRS provider, by the board and each of its employees. Identifying information shall include a subscriber's:
(a) Name;
(b) Telephone number; and
(c) Billing address;
(2) A CMRS provider, PSAP, or local exchange carrier (LEC) shall explicitly and clearly mark as confidential, prior to submission, information supplied and regarded by the provider, PSAP, or LEC as proprietary.
(3) The board shall not regard as confidential or proprietary the identification of a provider or LEC or a subsidiary of either.

Section 2. Allowable Uses of Confidential and Proprietary Information. The use of confidential or proprietary information shall be strictly limited to:
(1) Disburse funds as provided in KRS 65.7631(1), (2), (3), and (4);
(2) Discharge the duties of the board and its agents as provided in KRS 65.7629(1), (3), (8), (12), and (13)(a);
(3) Process revenues remitted to the board by CMRS providers; and
(4) Manage calls by PSAPs in accordance with KRS 65.7639.

Section 3. Management of Confidential and Proprietary Information in the Possession of the Board. (1) The board shall instruct, in writing, all board personnel, agents of the board, and PSAPs as to the proper management and uses of confidential and proprietary information.
(2) A nondisclosure agreement shall be signed by each board member, employee, and agent of the board who may handle or possess information deemed confidential or proprietary.
(3) Material deemed confidential or proprietary shall be specifically and clearly identified by the board.
(4) Only persons specifically authorized by the board shall open board correspondence. Correspondence received by postal mail, electronic mail, or facsimile and opened by an unauthorized person shall:
(a) Not be copied;
(b) Be immediately returned to its container; and
(c) Immediately forwarded to the board.
(5) Proprietary and confidential information in the possession of the board, a member, agent, or any other person or entity shall be stored in a secure room, vault, or container. The room, vault, or

container shall be kept locked when unattended or outside of normal business hours. Electronic files containing confidential or proprietary information shall be secured utilizing established mainframe protocols, stand alone servers, secured sockets, or password protected desktop applications, as appropriate.

(6) Access to confidential and proprietary information shall be limited to persons specifically authorized by KRS 65.7639.

(7) Each copy of confidential or proprietary information may be distributed as necessary for the efficient discharge of board duties and responsibilities.

(a) Copies shall be explicitly and clearly marked as confidential.

(b) A person possessing copies of documents containing confidential or proprietary information shall be responsible for document security.

(c) A copy no longer required shall be:

1. Returned to the board immediately; or

2. Destroyed immediately in such a manner as to prevent its reconstruction.

(8) An original record or file no longer needed for processing shall be:

(a) Sealed securely, retaining the notice of confidentiality, and transferred:

1. To a facility accessible only to the board administrator; or

2. With board approval, to the state archival and record storage center;

(b) With board approval, destroyed; or

(c) Returned to the proprietor.

Section 4. Breaches of Security. (1) The board shall take immediate action to determine the cause, impact, and persons involved in a security violation of the confidential information entrusted to the board.

(2) Unauthorized access to confidential or proprietary information shall be promptly reported to the board in writing.

(3) A report of a security breach shall include a description of the incident, specific identification of the information disclosed, identification of each person who accessed the records, and the purposes for which access was obtained.

(4) The board shall notify an affected party immediately, providing a copy of the written report detailing the incident.

(5) A board member, agent, or employee who willfully or negligently disregards a provision of this administrative regulation shall be dismissed or requested to resign.

(6) If a PSAP or its employee willfully or negligently disregards a provision of this administrative regulation, the board shall decertify the PSAP.

(7) A board member, agent, or employee who has been dismissed or asked to resign for willful or negligent disregard of the provisions of this administrative regulation may appeal the dismissal in accordance with KRS Chapter 13B.

(8) A PSAP that has been decertified for willful or negligent disregard of the provisions of this administrative regulation may appeal the decertification in accordance with KRS Chapter 13B. (26 Ky.R. 2108; Am. 27 Ky.R. 70; 1771; eff. 12-7-2000; 33 Ky.R. 4217; 34 Ky.R. 235; eff. 8-31-07.)